Attachment J.23

CDC & ATSDR
NETWARE 5 ARCHITECTURE
AND IMPLEMENTATION PLAN

Table of Contents

NetWare 5 Background & Advantages

Strictly speaking NetWare 5 is an enhanced version of the NetWare Network Operating System that provides advantages such as Pure-IP networking, Server Side Java support, NSS (Novell Storage Services) an improved volume type for supporting and quickly mounting very large volumes (8 terabyte file size and billions of files/directories) and quicker remounts (3 terabyte volume was crashed and recovered in 10 seconds at Comdex '97), Novell Licensing Services (an improved directory based licensing method), a faster, more scalable, Novell Directory Services version, tight integration of DHCP and DNS services with Dynamic DNS, and Novell Distributed Printing Services to better manage not only printers, but printer drivers as well. Additionally, companion products such as Z.E.N. Works (Zero Effort Networking), Migration Gateway, a JAVA-based NetWare Administration Utility (Console One), ORACLE 8 for NetWare, and Netscape Fastrack HTTP server are available.

Overview

This document examines the NetWare 5 deployment in three sections:

* Phase I - Infrastructure preparation.
* Phase II - Transition items for Pure-IP networking.
* Phase III - Migration Agents.

Phase I focuses on creating the infrastructure to transition all NetWare-based management to a Pure-IP network, including file, printer, application sharing and work station management. This phase:

* Lists the steps for NetWare 5 introduction to the current NetWare 4 tree.
* Establishes the architecture for using IP only service protocols.
* Sets the standard for converting NetWare 4 servers to NetWare 5.

Phase II focuses on the steps necessary to complete the transition to Pure-IP networking. This phase finishes with the disabling of IPX routing from all routing devices on all networks. To complete phase II, all NetWare servers on the CDC network must be running NetWare 5. Phase II should be completed by December 31, 2000 (12/31/2000).

Phase III focuses on Migration Agents (MA's). This phase is not part of the critical conversion path to a Pure-IP network. Phase III can be implemented as soon as NetWare 5 is introduced into the tree.

In summary, this document focuses in detail on phase I-infrastructure preparation, and on phase III-migration agents, with general guidance given for phase II-transition items for pure-IP networking. Before beginning Phase I, all LAN administrators must have taken the Novell 4.11 to 5.0 Update course #529 from a Novell-certified instructor.

Phase I

Overview

Phase I focus on creating the infrastructure to transition all NetWare-based management to a Pure-IP network, including file, printer, application sharing and work station management. This phase:

* Lists the steps for NetWare 5 introduction to the current NetWare 4 tree.
* Establishes the architecture for using IP only service protocols.
* Sets standards for converting NetWare 4 servers to NetWare 5.

Phase I documentation contains eight sections:

* Overview and Training.

* Preparation.
* The first server.
* Introducing NetWare 5 to all replica rings.
* Establishing an IP only service location protocol infrastructure.
* NetWare 4 to NetWare 5 upgrade standards and caveats.
* Novell Licensing Services.
* DHCP and Dynamic DNS integration with Novell Directory Services (NDS).

Training

It is required that all LAN administrators have at a minimum the Novell 4.11 to 5.0 Update Course #529 training from a Novell-certified instructor before attempting to install, upgrade and/or manage a NetWare 5 server. Prior to managing NDS objects such as users and printers an administrator should have completed the currently offered NetWare System Administration course.

It is highly recommended that annual training on at least one topic related to Novell 4.x or 5.x be taken by each LAN Administrator.

Phase I

Preparation

Server preparation

The NetWare 5 introduction to the tree extends the Novell Directory Services (NDS) Schema. Therefore, it is essential that all servers in the tree meet the following prerequisites:

* All servers need to have applied at least Intra NetWare support pack 5B.
* Directory service's version must be upgraded to Directory Services Version 6.03.

Both service packs are available on the CDC Novell Support Site. It is necessary that servers in the CDC-NDS tree meet these two criteria prior to the introduction of NetWare 5 into the tree.

Workstation preparation

Workstations must meet the currently recommended NetWare clients' version to connect to the servers using TCP/IP.

The currently recommended NetWare clients' versions are:

* 3.1 for Win 95/98.
* 4.6 for NT 4.

Note: NetWare clients prior to versions 2.5 and 4.11b will not work if they connect to a NetWare 5 server.

Workstations that do not have at a minium (previous CDC standard) NetWare version 2.5 for Win 95/98 or 4.11b for Win NT need to have a preferred server set to a NetWare 4.11 server.

Workstations running Win95 with the MS client and NDS services will be able to login but only over IPX/SPX. The MS NT4 using SP4 client will not login to a NetWare 5 server. This client is not on the CDC standard's list.

Phase I

First server upgrade

A NetWare 4.11 server holding only a read/write replica of the root partition will be upgraded to NetWare 5 using the in place upgrade method. This helps to ensure a smooth upgrade and therefore a complete introduction of the schema extensions into the existing tree.

Note: Once the master replica of any partition has been placed on a NetWare 5 server it cannot be put back on a NetWare 4.x server.

During the process of introducing NetWare 5 to the tree care must be taken not to place master partitions on any NetWare 5 server until the upgrade process is completed

To migrate the server to NetWare 5:

* Use the software installed on UOPS-XDV-INSTALL\vol1:nw5.
* Apply NetWare 5 Support Pack 2a.
* Apply timesync.nlm version 5.12.

Now the server will be downed and restarted. The extensions will then be allowed to propagate to all replicas for a period of approximately 12 hours.

Phase I

Introducing NetWare 5 to all replica rings

After the propagation period of approximately 12 hours, synchronization checks will be performed to establish the health of the NDS tree.

The next step is to upgrade the five (5) major NDS core master servers using the in place upgrade process. This will introduce a NetWare 5 server to nearly every replica ring at CDC. After one week the replicas on the NDS core servers will be promoted to masters again.

Note: After the replicas on the NDS core servers are promoted to masters, the NetWare 5 can no longer be removed from the tree.

Phase I

Establishing an IP only Service Location Protocol (SLP) Infrastructure

Background

Currently all NetWare services at CDC/ATSDR use RIP as a network routing protocol and SAP as a service location protocol, and both use IPX/SPX as the transport. There are over 2200 services registered with Novell for use over IPX/SPX with SAP. Every device on the network that makes services available through NetWare protocols uses SAP to announce it's availability and allow it to be found on the network. The dedicated network routers participate in the SAP process to propagate service availability information throughout CDC's networks. The majority of these are file-server-based file, printer and backup services. Although any network device can advertise services via SAP, i.e., a WIN95 workstation with a HTML editor software installed.

In order to transition to a Pure-IP environment, another method must be established for locating services on the network. Novell has implemented Service Location Protocol (SLP) - RFC 2165 over standard TCP/IP for server to server service location in the network.

SLP

SLP was chosen over DNS because it is a protocol designed for the discovery of services, not just a name resolution service. An illustration of the difference would be the ability of a client to query on a service type and receive a list of providers of that type as the reply. The CDC SLP architecture is designed to maximize redundancy, be manageable, offer good performance, and be conservative with network bandwidth.

How does SLP find resources?

SLP can use several methods in the process of finding resources. The available methods are:

* Static tables.
* DHCP.
* Directory Agent (DA) service.
* Multicasting.
* Broadcasting.

Server visibility

All servers will be visible to all users at CDC. Other services that advertise via SLP will be visible grouped by and CIO by using scopes.

Primary method of service location

The primary method of service location will be through the use of the DA server agent. Each client will be configured to use DA's and then DNS for service location. The client will first query the local Campus DA, if that is not found it will go through a list of up to four other DA's until it finds one or reaches the end of the list. If no DA is found then the client will attempt to multicast to find the service.

With five DA's in Atlanta the only time one would not be available would be if the local DA had failed and the campus link is down. If the campus link is down then local services are the only ones that are at issue, multicasting will reach them. If multicasting cannot be configured or has failed on a campus due to hardware issues then DNS will be queried by the client. Any server that is entered in the DNS will be resolvable with a standard DNS query. Each DA will also run a DNS process providing local and redundant DNS services, not only for NetWare, but for all DNS resolved services. The DNS and DA tables are populated through separate processes and so it would be possible for an improperly configured server not to be visible in one service list but be available in the other providing further redundancy. The blocking of the NetWare multicasting address will ensure that multicasting traffic will not be an issue between campuses.

Multicasting recommendations

It is recommended that multicasting be enabled on each local campus but the NetWare multicast addresses be blocked from crossing inter-campus links. This will provide a redundant method for finding all local resources if there are no DA's available.

Service scope definition

Another new concept is that of service scopes. A scope is a logical collection of resources such as servers and printers that are visible as a group. Every SLP service must be registered with a scope to be visible from a DA.

Service scope recommendations and registrations

The recommendation is that there be one scope at CDC called "CDC-NW-Services" that all servers will register with. In addition at each campus each CIO will create a scope following the convention of "CIO-Campus."

All of the CIO campus resources except servers will be registered in that scope. Each client will be configured to query first the "CDC-NW-Services" scope and then the "CIO-Campus" scope. This will ensure that each client will see all the locally available resources from within the CIO and be able to see all servers across CDC as well. Clients can be configured to look in up to five scopes if additional resources need to be seen.

The RFC for SLP provides for registration of services with the DA servers. All NetWare 5 servers at CDC should be statically configured to populate both the local and two remote DA's. Depending on the size of the campus and scope there may need to be one or more partitions dedicated to holding the scope data. The NDS Help desk will coordinate which off campus DA will carry which scope since this must match both the partition that the scope will be in and the rollout sequence for the DA's.

DA-DNS Servers introduction

A DA-DNS Server will be introduced to each of the major campuses. These servers will be used as the core DA servers. These servers will be located at each of the major geographic campuses: Koger, Clifton, Corporate, Executive and Chamblee in the Atlanta area. These servers will provide DA and DNS support as discussed previously.

Remote Sites

Greater than 100 users

The first NetWare 5 Server at remote sites with greater than 100 users will be required to have a DA installed as well. These sites must convert as their first NetWare 5 server one that can serve as the DA in addition to its current duties. DA installation at the remote sites should be coordinated with the NDS help desk.

Less than 100 users

Remote sites smaller than 100 users: Washington, D.C.; Alaska and Spokane, will not be required to run a DA. These smaller sites should be able to successfully revert to multicast location of services in the event of WAN failure on the assumption that their sites do not incorporate routers locally.

Phase I

NetWare 4 to NetWare 5 upgrade standards and caveats

Additional NetWare 5 servers will only be installed after the core NDS master replica holders have been upgraded. NetWare 5 servers installed will have support pack 2a and timesync.nlm 5.12 installed at the time of upgrade.

Timesync

Current timesync relies on IPX. As servers are upgraded to NetWare 5, they will be configured to utilize an IP-based time synchronization transport.

Primary time servers and backup time servers

The Atlanta campus DA's will be the primary time server's participating with the existing time servers as well. All subsequent NetWare 5 servers on a campus will be secondary time servers and list the Campus DA as their first configured time source. A locally administered NetWare 5 server will be designated as a campus backup time server, obtaining its time from the local campus DA first and with an off-campus source second in its configured source list. It will be listed as the second configured time source for all other NetWare 5 servers at that campus.

Dual protocol stacks

All NetWare 5 servers will run dual protocol stacks until Phase II is completed. This will help to prevent service location failures in a mixed NetWare 4 and NetWare 5 tree during transition. As more printers and workstations are converted to utilize SLP, IPX traffic will diminish on the network.

Drivers

NetWare .dsk drivers are not utilized under NetWare 5. Prior to upgrading be sure you have a NetWare 5 .ham module available for your subsystem. The

NDS help desk can check the list of modules that come with NetWare 5 or the device manufacturer's web site can be consulted.

Upgrade standards

All workstations serviced by a particular NetWare 5 server should be upgraded to the latest approved NetWare client version. Currently the latest approved versions are:

* ò3.1 for Windows 95/98.
* ò4.6 for Windows NT.

Client tailoring

Clients that are running the latest NetWare client software can take advantage of advanced features to configure DA, preferred server, and scope information that is essential to enabling the workstation to utilize server based services via Pure-IP. The latest clients also enable configuration options such as SLP utilization preference that allows tailoring the client for best performance. This tailoring is essential for maintaining performance on the workstation as servers are converted to NetWare 5.

Note: Recommendations for performance tailoring can be found on the Intranet pages for NetWare 5.

Login scripts

All login scripts that do not already use distinguished NDS names for volume map objects, printer objects, attach commands, etc., should be modified to do so. Distinguished NDS names are necessary for NDS-based resource location utilizing SLP. All hard coded resource references should be updated before IPX and SAP can be removed from the network.

Novell Storage Services option

Novell Storage Services offer an enhanced volume type for storing many or particularly large files. Additionally, they remount exceptionally quickly compared to standard Novell volumes. As soon as a server is upgraded to NetWare 5, a CIO may choose to take advantage of this technology.

Novell Storage Services limitations

Some limitations to note are that the NSS volume will not support compression, sub-allocation, or the transaction tracking system (TTS). A server sys: volume cannot be NSS. A separate utility is provided with

NetWare 5 to repair NSS volumes. Fault tolerance for NSS volumes must be a hardware implementation, as software RAID is not available for this type of volume under NetWare 5. As with all NetWare volumes adding server memory above the minimum required to mount a volume will provide performance benefits. This is particularly true of NSS since it can mount huge volumes with just a few megabytes of memory. Particular care should be taken when migrating from traditional NetWare volumes to NSS volumes. If data is backed up in compressed form from the traditional file system it cannot be restored to an NSS file system because NSS does not support disk compression.

Phase I

Novell Licensing Services

Novell Licensing Services (NLS) was created to help control and monitor the use of licensed software. NLS store licensing information in NDS. NetWare 5 use is controlled through NLS. The licensing information is in the form of a license certificate envelope that contains two types of certificates: Server base license certificate(s) and Server connection license certificate(s). This requires that the NDS schema be extended to accommodate these new object types. The schema will be extended when the first NetWare 5 server is introduced to the tree.

Master Licensing Agreement (MLA) and license certificates

CDC maintains a Master Licensing Agreement (MLA) with Novell for NetWare software. The MLA licensing envelope contains an unlimited Server base license certificate and an unlimited Server connection license certificate. By default a server upgraded to NetWare 5 will search the tree all the way to the root if necessary to find a license certificate. Once found, the server will load the license in memory for quick access. Because these licenses are unlimited, they should not be assigned to specific servers as is usually done. Doing so will prevent servers that would later attempt to use them from obtaining licensing. Do not assign servers to these certificates.

When the first NetWare 5 server is added to each partition in the CDC-NDS tree, a license envelope will be installed at the root of that partition, thereby ensuring that any subsequent NetWare 5 servers have access to unlimited server and unlimited connection license certificates. For performance purposes, a license certification should be installed in each partition where NetWare 5 servers will be installed.

First server certificate

Certificates will be added when the first server in a partition is upgraded to NetWare 5. The NDS Help Desk should be contacted for a copy of the MLA license diskette needed during the NetWare 5 installation.

Subsequent servers

All subsequent servers in that partition need only add the cryptographic foundation key. During the NetWare 5 installation select to Install without License. Then copy the cryptographic foundation key file to the sys:system directory on the server. The file is called NICIFK . It is available from UOPS-XDV-INSTALL/VOL1:nw5/license . Contact the NDS Help Desk for userid/password access to the server.

Installation from UOPS-XDV-INSTALL/VOL1:nw5

If you are installing NetWare 5 from UOPS-XDV-INSTALL/VOL1:nw5, then the cryptographic foundation key file has already been added. For information about using UOPS-XDV-INSTALL for installation of NetWare 5, contact the NDS Help Desk.

Phase I

DHCP and Dynamic DNS integrated with NDS

IP address management

It is recommended that DHCP be utilized for IP address management, and a DHCP server that have extensible option tags be used, i.e., SUN Solaris DHCP server or NetWare 5 DHCP server.

Option tags

Option tags to provide preferred server, DA's and scope can be added to an extensible DHCP server. This greatly simplifies a manual configuration on workstations to enable them to communicate properly on the network as the servers they utilize are converted to NetWare 5. The preferred server option tag should be set to a server carrying a replica that contains the users-ID, DA should be configured with the DA rollout defined for that campus, and the scopes should be set to "CDC-NW-Services" and "CIO-Campus" in that order.

Server IP address

As NetWare Servers are converted to NetWare 5, they will require an IP address if they do not already have one. All NetWare 5 servers should be

registered in the DNS. As clients are configured to utilize the Pure-IP environment, they should be set up to utilize DNS in the event of SLP failure. Currently RIP/SAP is our only service location protocol for NetWare resources.

Primary service location protocol

With the upgrade to NetWare 5, SLP will serve as the primary service location protocol and DNS as the backup. DNS running on NetWare 5 implements the standard DNS functionality. It also implements Dynamic DNS integrated with NDS. As workstations are given IP addresses via NetWare 5 DHCP servers, the DHCP server can feed the DNS server the information to register the workstation name and IP address. The DNS records are stored in an NDS object and therefore propagated throughout the NDS replica ring containing the object.

DNS service

CDC/ATSDR maintains a DNS service both outside and inside the Internet firewall for security purposes. The inside DNS service should be moved to NetWare to facilitate distributed internal manual registrations, provide for redundancy for DNS lookup, create a distributed DNS lookup capability and take advantage of dynamic DNS registration of workstations wherever useful.

The DA servers will be configured to provide DNS services for inside registration. Workstations should be configured to utilize its campus DA-DNS server. If the workstation IP address is obtained using DHCP, it is strongly recommended that the proper DNS server be provided automatically. This architecture will provide for fault tolerance in the event of MAN failure, distribute the workload of DNS lookup and localize DNS lookup traffic on the network.

Phase II

Identifying IPX dependencies

Infrastructure minimums

Phase Two can only be completed when:

* SLP infrastructure is established.
* All Servers are upgraded to NetWare 5.

This includes ensuring all clients are running at least:

* 3.1 for Windows 95/98.
* 4.6 for Windows NT.

This is essential to complete the Phase Two steps to remove IPX from the network. All workstations and servers must be configured for Pure-IP support at this point.

IPX/SPX service identification

All services that are limited to IPX/SPX for transport and advertisement must be identified. The most widely distributed application of this type is the current mainframe gateway, though there are others. Once all such applications are identified and upgraded or replaced IPX/SPX routing can be disabled. Many IPX/SPX dependancies will be eliminated during normal product upgrades as most vendors are moving to TCP/IP for transport.

Phase II

Configure all printers to be IP only

In order to eliminate IPX, all NetWare queue-based, printing must be converted to an IP only method of printing. This can be accomplished by one of two methods. The methods are:

* Line Printer Daemon (LPD).
* Novell Distributed Printing Service (NDPS).

Printing communications consists of two pieces: client-server communication and server-printer communication.

Line Printer Daemon (LPD) printing method

LPD was originally a UNIX-based printing method. The printers were all host-attached and clients would communicate with the host and the host would print to a directly attached printer. Over time, LPD network devices were developed for printers that have minimum host functionality on the Network Interface, so communication appears to be client-printer. This standard has been around for a long time and most direct network attached printers will support LPD. If the LPD is used to poll the server-based print queue, the server will spool the print job. When it is used to print directly to the printer, the workstation is responsible for queuing and formatting the print job.

Novell Distributed Print Services (NDPS) printing method

NDPS are a new printing facility available with NetWare 5. NDPS have the advantage of allowing central management of printer drivers and bidirectional communication between the server and printer. Printer drivers are installed to the printer object and distributed automatically as needed to workstations. Job status information and control is enhanced by bidirectional communication with the printers over the network. Print jobs are spooled on the server to a waiting printer. To take full advantage of NDPS features, a printer must be NDPS compliant. NDPS compliant printers are available from XEROX, CANON, and HP. All shared printer purchases should require NDPS compatibility.

Non-NDPS compliant printers

Non-NDPS compliant printers that support LPD can still be defined to NDPS to take advantage of automatic printer driver distribution and server queuing of print jobs. Availability of status information and control for administration is not fully featured as with an NDPS compliant printer.

Phase II

Check Timesync over IP Configuration

As each server is upgraded to NetWare 5 its time synchronization configuration should have been modified to move it to IP only time synchronization. Since time synchronization is essential to Directory Services health, It is important to check all server time synchronization before turning off the IPX time server sources.

Post Phase One, the NDS help desk will announce the intention to turn off the IPX time servers on a specific date. CIO's will be responsible for ensuring their servers time configuration is up-to-date by that date.

Phase III

Migration Agents

Migration Agents allow IP only clients to utilize resources that are only available via IPX. A direct network attached client running a current NetWare client does not need this type of service as it can directly access resources using either IP or IPX because all NetWare 5 servers at CDC will run dual stacks. In the CDC/ATSDR environment the Migration Agents are useful for utilizing IPX only resources via an IP only dial-up connection. Migration Agents can be installed as needed for this type of access. Specific guidelines must be followed to prevent routing issues.

Migration Agents can participate in a virtual network between themselves

over the network for purposes of service location and utilization. The Migration Agents are included in a virtual network by assigning a common CMD network number. All Migration Agents with the same CMD network number will then route over the virtual network and advertise services to each other using NLSP (Novell Link State Protocol). In order to prevent the possibility of the virtual network erroneously becoming the shortest path for normal IPX network traffic, each MA should be assigned its own CMD network number. Since normal RIP/SAP traffic will make NetWare resources available from the whole MAN, there is no need to create a virtual network between MA's.

One exception can be allowed. If multiple MA's are needed in a CIO and will be located on the same LAN (no routing devices between them), then they can share a CMD network number because there will be no routing occurring between them anyway.

The convention for CMD network numbers will be to use IPX network numbers that follow the existing CDC conventions.

Notification of the installation of a MA including CMD network number should be sent to the NDS help desk for tracking purposes. The NDS help desk will maintain a list of installed MA's for possible troubleshooting purposes.

Time line of Major Milestones & Responsibilities

Event	Completion Date	Responsibility
All Servers on Support Pack 5B or > DS 6.03	6/28/1999	NTB
Designate replicas other than on the Core NDS Servers in NTB as Masters for Each Replica Ring	6/28/1999	NTB
Upgrade read/write root replica holder to NetWare 5 to extend schema	7/9/1999	NTB
All CIO's		
Workstations on Standard Clients		
Install read/write root replica holder 4.11 server for safe		
Upgrade Core NDS Servers in NTB for quick NetWare 5		

95/98 on 2.5 or >	schema extension of CDC-NDS tree	introduction into most replica rings
NT on 4.11b or >		7/10/1999
current CDC standard	7/8/1999	NTB
	NTB	
All CIO's		
Install DA's on Major Campuses	completed by	Resolve all IPX Dependencies1
12/31/2000	10/1/2000	
Week of 7/12/99	12/31/2000	10/1/2000
NTB	All CIO's	All CIO's
Install DA's at remote sites	Check Timesync over IP	Configure All Printers to be IP only
When CIO ready	7/1/2000	11/1/2000
	All CIO's	All CIO's
CIO &NTB	Identify IPX Dependencies	Begin IPX routing shut off
Inside DNS moved to Novell DNS	8/1/2000	11/15/2001
	All CIOs	NTB
To be determined		
NTB		Finish IPX routing shut off
	Update Login Scripts 10/1/2000	
Remaining 200+ servers upgraded to Netware 5	All CIOs	NTB
	Resolve all IPX	

Server configuration and management

File compression

It is strongly recommended that the SYS volume contain only the operating system files and that file compression and suballocation should be turned off. If it is not possible, then file compression and suballocation should be turned off on the SYS volume unless FILER is used to flag directory structures so that no more than 90% of the volume space is used by all directories on the volume. It is critical that there be at least 10% free space and a minimum of 1000 free blocks on the volume to prevent decompression from interfering with the OS operation.

Suballocation

The following are recommendations from Novell and the CDC standard when disk suballocation is enabled:

* Use a disk block size of 64K on all volumes where suballocation is enabled. This is the fastest and most efficient block size for volumes with suballocation enabled.

* Keep 10%-20% of the volume space free to avoid the suballocation "Aggressive" mode. Disk space management is essential to avoid problems with suballocation. Make sure there is always 10%-20% available disk space on all volumes. This can be monitored by SERVMAN.NLM, NWADMIN.EXE or NDIR /VOL. If you are running low on disk space you need to either delete unneeded files or add additional disk space to the volume.

* Maintain a minimum of 1000 free blocks on each NetWare volume that has suballocation enabled.

* Suballocation uses free blocks to perform its function. When free blocks are low suballocation could go into "aggressive" mode, lock the volume and cause high utilization. Maintaining over 1000 free blocks will avoid this problem in most cases. If there are not at least 1000 free blocks on the volume, run a PURGE /ALL from the root of the volume. This will free the "freeable limbo blocks" and move them back to "free blocks."

Set PURGE flag on all directories that have large amounts of temporary files created. Every temporary file that is created will be put on the "deleted file list." These files are kept on the disk until a PURGE is run. In order to avoid disk space and free block problems, you need to set the

PURGE flag on specific directories that create large numbers of temporary files. Also, setting IMMEDIATE PURGE OF DELETED FILES=ON will avoid this problem. It is important to note that using the purge flag on selected directories precludes salvaging file from the directories for which the option is set. The other option affects all volumes on the server and should be used with full acceptance of the recovery implications.

Auditing

Auditing means examining records to make sure that transactions are accurate and that confidential information is secure.

NetWare auditing allows each CIO Information Services Security Officer (ISSO) to act independently of the container administrator or network supervisor to audit network transactions.

The ISSO can audit NetWare Directory Services events, as well as those specific to a volume file system or a server.

Auditors can track events and activities on the network, but they do not have rights to open or modify network files (other than the audit data and audit history files), unless they are granted rights by the network supervisor.

Auditing is enabled at the volume level for file system auditing. It is enabled at the container level for NetWare Directory Services auditing.

Auditing for the purposes of monitoring activities performed by administrators in the corporate environment, including CIO containers, is a necessary and important part of overall operations of the system. Auditing should capture all events with potential system implication, all accesses to highly sensitive data stores (e.g., personnel data, some procurement data, identifiable medical data, etc.), and perhaps other items. Audit trails will be made available to the appropriate ISSO.

Required Directory Services Auditing:

Audit by DS events

Add Partition

Add Replica

Change ACL

Change Password

Change Replica Type

Disable User Account

Enable User Account

Intruder Lockout Change

Join Partitions

Remove Partitions

Remove Replica

Split Partition

Audit by User

Container Administrators and manager accounts

Minimum Volume Auditing:

Audit by File Event

Delete Directory - global

File Salvage

Audit by Server Events

Change Date/Time

Down Server

Volume Dismount

Volume Mount

Audit by User Events

Disable Account

Audit by User

Container Administrator

The above are minimum standards. ARM staff in each CIO will need to evaluate their environment to determine if more auditing needs to be performed (for instance, auditing all access to confidential information.)

Backup software

To properly backup both the NDS and the file system, Novell recommends that you use applications which fully support the SMS architecture. The software used should utilize Novell's TSANDS.nlm to backup the NDS, and TSA50.nlm to backup the file system. The following backup software has been tested

* Cheyenne Software ARCserve for NetWare V6.6.
* Seagate Backup Exec ver 8.0.

It is important to note that although prior versions of backup software may back up the data on a NetWare 5 server, it may not properly backup the NDS and associated file system trustee rights.

Traditional print queues NetWare 5 cannot be backed up properly, and must be recreated if lost.

Because no LAN administrator will have rights to the entire directory structure, NTB will backup the entire NDS on a weekly basis.

Caution: The health of the NDS must depend on replication, as opposed to backup. The backup of the NDS does not include partition or replication information. Restoration of any part of the NDS from tape backup should be a last resort, and will not be performed without the concurrence of the tree management group.

Client software

Please refer to the CDC LAN Standard's document.

Hardware standards

Servers running NetWare should have a Pentium processor running at a minium of 66MHz. If the NDS is being impacted by the processor speed on a server the replicas in question may have to be removed until a faster processor can be installed. NDS services are visibly faster with faster CPU's, one slow CPU in a replica ring will make a visible difference in NDS operations. Any server containing a replica copy must have the SYS volume either duplexed or protected by some type of fault tolerant RAID system. It should be kept in mind that the compression and decompression speeds are related to processor speed. File decompression speed for large files is impacted by disk subsystem speed since the entire file is decompressed and

is written back to disk. NDS synchronization speed for servers with large replicas is impacted by disk speed as well since updates are made to the disk during this process. New DOS partitions should be at a minium 600 Mb, one Gig recommenced. The system partition should be at a minium one Gig and where possible more with two to three Gig not being unreasonable.

Memory is very important to NetWare server stability. Any server with a replica copy must maintain a minimum of 65% free cache buffers as reported by the server monitor screen under the resources section. Servers not meeting this requirement must not have a replica placed on them, servers dropping below 60% should have any replicas removed. Auditing of these limits with automatic reporting to the tree management team will be instituted.

NDS software revision control

The minimum NDS software revision will be identified by NTB. The time limit for updating the software will be determined at the time a new minimum revision is identified. No NDS software may be updated without the concurrence of the tree management group.

CDC NDS naming standards

Organization and Organizational Unit Names: The Organization and Organizational Unit names will be based on standard CDC abbreviations of our unit names. For example, Organization is CDC, CIO is NCID and division is OD. Thus, the context in the corporate tree is OU=OD.OU=NCID.O=CDC.

Server Names: The current standards for naming file servers will be maintained.

Printer Names: Printer names will start with the characters PR.

Print Server and Print Queue Names: Print server and print queue names will start with the characters PS and PQ, respectively.

Group Names: Group names will start with the characters GP. The rest of the name will be based on the function performed by the group. For example, GP-Budget.

Organizational Role Names: Organization role names will begin with the characters OR.

Profile Names: Profile names will start with the characters PF. The rest of the name will be based on the function supplied by the profile. For example, the profile in a container providing all the required mappings for

a division would be named PF-divnameMAP.

Directory Map Names: Directory map names will begin with the characters DM. The rest of the name will be based on the application or process being mapped. For example, WordPerfect application files could be mapped with a Directory Map named DM-WP.

Bindery emulation/bindery issues

Bindery Services allows Directory Services to emulate a bindery. The reasons to do this are mostly oriented in support of software requirements that necessitate interaction with the Novell Bindery objects. Some instances where this might be required include print server software, and backup software.

Bindery Services is enabled when the Bindery Context is set. In general terms, the Bindery context is set within an 'Organization' object or within an 'Organizational Unit' object in the NDS tree structure. All objects within that container object are then emulated in a flat bindery manner. The names of those objects must be bindery compatible, i.e., no spaces or other special names that are only allowable only in NetWare NDS objects. Any sub-containers within the bindery emulated container do not have bindery emulation 'carried forward'. NetWare allows up to 16 bindery contexts to be set within a particular server environment. Experience seems to show that certain software requires that the Bindery objects be defined particularly within the first Bindery Context that is SET. This can be done with a 'SET BINDERY CONTEXT=.....' command from the server console or permanently placed in the AUTOEXEC.NCF server startup file.

One important implication in Bindery Emulation is that a Bindery Context can only be set if the server holds a writeable (meaning master or read/write) replica of the partition to which the Bindery Context is being set. This means that if the Bindery Context is being set to the Organization Unit OU=IRMO.O=OPS and O=OPS is a Partition, then the server on which the context is being set must hold a writeable replica of the 'OPS' partition. By way of inference, this means that the placement of the Bindery Context (where it is SET in the NDS) also has implications for partitioning and replication design.

Regarding client interaction with the Bindery versus NetWare 4 NDS, a client variable called "NDS" will be 'SET' to "Y" in a user's login script to indicate if a client is in the native NDS environment, i.e., through a contextual login to the NDS tree. This allows CDC software, such as the REQUEST batch files, to easily test whether a client is either in a NetWare 3.x or NetWare 4 environment.

NDS & directory management rights

This section deals with the assigning of rights for management of both NDS objects and the file system. It does not outline how to manage your network resources but does provide guidelines to promote security and stability.

When assigning rights, consideration should be given not just to explicit rights but what that user can then do for itself. If a user is given rights to write to any property of an object, that user can then change his or her rights to that object. Any object should be presumed to have the maximum rights it can create for itself, not just what has been explicitly assigned.

Rights should be explicitly assigned to manage an object or directory. If, when assigning rights, it becomes necessary to block some of those rights at a lower level, the management strategy should be reviewed. In most cases, management can be setup in such a fashion that security is not dependent on revoking rights from specific objects. This eliminates the possibility of new objects being accessible to ID's not intended to have access.

Container objects will not be used to deliver directory rights or login scripts. Both these needs can be satisfied by the use of profiles and groups which do not have the liabilities associated with being able to write to the Container object.

The recommended method for granting rights to objects and directories for management purposes is through use of the Organizational Role (OR). Making an OR the trustee of an object will allow complete management of the object by any ID occupying the role. This makes it very easy to grant managerial rights to an ID in a consistent manner. Giving an OR the CREATE right to a container allows occupants of the role to create new objects at any time. Since the creator of an object is by default given supervisor rights to that object, the new object is completely manageable.

The Inherited Rights Filter (IRF) will not be used to block the flow of rights to container, server, or volume objects. The use of the IRF can render portions of the tree unmanageable and is not necessary to provide network security.

Partitioning management

Management of the NDS is the responsibility of the Network Technology Branch (NTB) of IRMO. There will be minimally two people fully familiar with the tree structure and its maintenance in NTB. Work schedules will be maintained so that one of these designated staff persons will always be

available locally to address system issues. The structure of the NDS partitions must be documented in writing, with a copy kept in printed or electronic form off site. There should always be at least one current printed copy available at all times. This document must be kept current with all changes made no later than the first full business day following a change. This documentation must include a listing of all partitions with the associated replica locations, and a second list of servers with the replicas on each server. The location should include the host servers' physical location, internal IPX number, TCP/IP address, contact person for that server and an alternate, where available. The console and rconsole password for every server that has a partition must be held by the group responsible for the partition or partitions on that server. These passwords will be used only for NDS maintenance purposes.

Prior to executing any upgrades, maintenance, or other NDS system work, the contact person for the server hosting the replica will be notified. The only exception to this should be if system stability and serviceability are in question and efforts to notify the contact person have been unsuccessful. If this exceptional situation occurs, then documentation of the situation, efforts made to contact others, all actions taken to rectify the situation, and any outstanding issues to be resolved must be written and sent to the contact person within one business day. System logs should be kept, recording upgrades and maintenance actions on each partition and server. Routine system maintenance should be scheduled to minimally impact customers, with notification to the affected administrators at least seven business days in advance. If a server is being taken down that has a replica on it, the group responsible for management of that partition must be notified. This notification must take place far enough in advance so removal of the replica is possible, should it be necessary. Maintenance of the partitions and replicas, including the use of Novell or third party maintenance tools such as DSREPAIR.NLM, will be done only by or at the instruction of the group responsible for the partition in question.

If a CIO wishes to assume responsibility for the partition functions in its branch of the tree it may do so. Management responsibility for partitions will not be delegated below the CIO level. CIOs managing their own partitions must meet the same requirements as the central support group. The central support group should be given a copy of the current document each time it is revised. The primary and second person responsible for partition maintenance should be identified to the central support group by the CIO. Contact procedures complete with necessary names and numbers should be furnished to the central support group so one of those persons can be contacted in the event system maintenance is necessary.

Any server with a replica on it must meet the hardware requirements found under the hardware section of this document. There should be three copies

of every partition. One of these partitions should reside in a separate geographical location so a single natural disaster will not compromise the integrity of the tree.

There are three reasons to create a new partition. If a partition has more than 5,000 objects, more than twelve copies exist of a replica, or to minimize traffic over a slow WAN link (T1 or less). Partitioning for reasons other than these should be avoided, but where desired, they will be discussed with the tree management group.

Notification procedures/request for support

IRMO would like to provide all of you with expedient NetWare support; proper notification procedures for LAN Administrators are listed below.

If you are experiencing critical NDS problems, call (404) 639-7800. The person answering your call will beep a member of the NetWare NDS Support team and you will get assistance immediately. Calling (404) 639-7800 insures that you will get a warm body to answer your call and alerts us that someone needs an immediate response.

If you are reporting a problem that does not require immediate assistance, or you are sending a notification, please send an E-mail to the NDSHelpDesk mailbox with detailed information. You should also use the help desk for response to any issues or questions you might have regarding the NDS this includes "quick questions." Calling with a quick question takes away time from those who use the help desk.

Schema management

The NDS schema in NetWare 5 is extendable. All extensions to the schema will be done by the central support group. Rights will not be given to individuals outside of the group even temporarily to make the extension. Groups needing extensions should coordinate with the central support group giving advance notice of the need. Prior to the CDC schema being extended several requirements should be met. The software used to extend the schema should be tested on the CDC WAN to demonstrate that it works properly. The vendor requiring the schema update should give written assurance that there are no conflicts with earlier versions of the software using the schema extension. It should be established that the extension will not be disruptive to those using an existing extension from the same vendor. Any conflicts should be identified and resolved in advance. Full testing of the software that is to use the software should have been done on test systems. Extensions should not be done unless the requesting group is sure that the software will meet their needs and be used.

Server Notification Procedures

When any server will be placed into or an existing server moved within the tree the support group responsible for that part of the tree will be notified at least twenty-four hours in advance. This notification will include the necessary information to document the server including the servers' physical location, context, internal IPX number, TCP/IP address, contact person for that server, an alternate, where available, and the rconsole password for any server that has a replica.

If a server is to be taken down for maintenance, the support group responsible for that part of the tree will be notified as much as possible in advance. If a server goes down or must be taken down without advance planning, the support group for that part of the tree should be notified the next business day.

These notification procedures will allow those responsible for the NDS health to correlate error logs with events, and minimize scheduling conflicts that may exist between mutually exclusive NDS activities.

Restraints on The Use of Global Tree Maintenance IDs

IRMO staff will be in sole possession of the IDs for global tree maintenance. The powers vested in these IDs will be used only for the purposes of performing maintenance of the network OS. If other functions or accesses are considered necessary under the power of these IDs, then formal proposals will be presented to and accepted by the ARM Coordinators prior to exercise of those authorities. In any case, all activity performed under these IDs will be recorded in an audit file which is under the exclusive control of the IRMO ISSO.